This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-27. (Cancelled).

28. (Previously Presented) A method for clustered Secure Sockets Layer (SSL) acceleration, comprising the steps of:

connecting at least two SSL relays in a cluster;

establishing a communication path between a first node and a second node via a first SSL relay of the cluster, wherein the communication path includes an SSL connection between the first node and the first SSL relay;

transferring information between the first node and the first SSL relay, wherein the transferred information relates to a communication from the first node to the second node and wherein the transferred information includes a record;

transferring the information between the first SSL relay and the second node; and

clustering state information of the communication path when the record has been acknowledged by the second node, the clustering comprising sharing the state information between the first SSL relay and at least a second SSL relay of the cluster, wherein the second SSL relay is capable of taking over communications between the first and second nodes upon failure of the first SSL relay.

29. (Previously Presented) The method according to claim 28, wherein the first node comprises a client and the second node comprises a server.

30. (Previously Presented) The method according to claim 28, further comprising transferring the information related to the communication between the first node and the second node to the second SSL relay transparently upon failure of the first SSL relay.

31. (Previously Presented) The method according to claim 28, further comprising transmitting the communication from the first node to the second SSL relay and from the second SSL relay to the second node transparently upon failure of the first SSL relay.

32. (Cancelled).

33. (Cancelled).

34. (Previously Presented) The method according to claim 28, further comprising sharing an SSL session cache across all of the at least two SSL relays.

35. (Previously Presented) The method according to claim 28, further comprising clustering an SSL session resumption between the first node and the first SSL relay.

36. (Previously Presented) The method according to claim 28, further comprising clustering cryptographic keying information across all of the at least two SSL relays.

37. (Previously Presented) The method according to claim 36, further comprising clustering a key and a current Cipher Block Chaining (CBC) residue.

38. (Previously Presented) The method according to claim 36, further comprising clustering a sequence number.

39. (Previously Presented) The method according to claim 36, further comprising clustering a current key schedule.

40. (Previously Presented) The method according to claim 36, further comprising clustering a key and an offset into a key stream.

41. (Previously Presented) The method according to claim 28, further comprising clustering a cipher state.

42. (Previously Presented) The method according to claim 28, further comprising clustering data from a partial record corresponding to data from either the first or second node.

43. (Previously Presented) The method according to claim 28, further comprising clustering an information size.

44. (Currently Amended) A system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node;

a second node; and

an SSL relay cluster for connecting the first node and the second node comprising:

a first SSL relay configured to cluster an SSL client handshake following reception of the SSL client handshake from the first node; and

a second SSL relay configured to transmit an acknowledgment to the first SSL relay after receiving update information from the first SSL relay,

wherein the first SSL relay is further configured to transmit a handshake acknowledgment message to the first node following reception of the acknowledgment from the second SSL relay.

45. (Previously Presented) The system according to claim 44, wherein the first node comprises a client and the second node comprises a server.

46. (Previously Presented) A computer readable medium storing computer readable instructions that, when executed by a processor, perform a method comprising:

establishing a connection between a first node and a second node via a first SSL relay of an SSL relay cluster, wherein said SSL relay cluster comprises at least two interconnected SSL

relays and wherein the connection includes an SSL connection between the first SSL relay and the first node;

receiving a data communication from the first node, wherein at least a portion of the data communication is structured as a record;

transmitting the data communication to the second node;

receiving a first acknowledgment from the second node, wherein the first acknowledgment acknowledges the record;

following reception of the first acknowledgment, clustering state information of the established connection with at least a second SSL relay of the SSL relay cluster; and

receiving a second acknowledgment from the at least second SSL relay in the SSL relay cluster confirming successful clustering.

47. (Previously Presented) The computer readable medium according to claim 46, wherein the second SSL relay assumes the first SSL relay's responsibilities upon failure of the first SSL relay.

48. (Previously Presented) The computer readable medium according to claim 46, wherein the first node comprises a client and the second node comprises a server.

49. (Previously Presented) An SSL relay, the SSL relay connected in a cluster of SSL relays, comprising:

a first interface for transferring information between a first node and the SSL relay, wherein the first interface includes an SSL connection between the first node and the SSL relay and wherein the information includes record formatted data;

a second interface for transferring the information between a second node and the SSL relay;

a third interface for transferring state information between SSL relays in the cluster when the record formatted data has been acknowledged by the second node; and

a storage device, wherein state information of an SSL connection between the first node and the SSL relay is shared across each SSL relay in the cluster, any of the SSL relays in the

cluster capable of taking over all connections of another SSL relay in the cluster, wherein the storage device is further configured to store the transferred information in a queue until acknowledgement is received from the second node.

50. (Previously Presented) The SSL relay according to claim 49, wherein the first node is a client and the second node is a server.

51. (Previously Presented) The SSL relay according to claim 49, wherein the first interface and the second interface are the same.

52. (Previously Presented) The SSL relay according to claim 49, wherein the second interface and the third interface are the same.

53. (Previously Presented) The SSL relay according to claim 49, wherein the first interface and the third interface are the same.

54. (Previously Presented) The SSL relay according to claim 49, wherein the first interface and the second interface and the third interface are the same.

55. (Previously Presented) The method of claim 28, further including the steps of:

setting a timer when the record is read, wherein the record is a partial record; and

clustering the partial record if the timer expires.

56. (Previously Presented) The method of claim 55, wherein the timer corresponds to two times a packet interval time.

57. (Previously Presented) The method of claim 28, further including the step of storing an unacknowledged portion of the information transferred between the first SSL relay and the second node in a queue.

58. (Previously Presented) The method of claim 57, wherein the unacknowledged portion of the information transferred between the first SSL relay and the second node is stored in the queue with a cipher state associated with the information.

59. (Previously Presented) The system of claim 44, wherein the update information includes at least one of: a new TCP state, a current value of SSL handshake hashes and a handshake to enter upon failover.

60. (Previously Presented) The system of claim 44, wherein the handshake acknowledgement message includes at least one of a server handshake and a server handshake completion message.

61. (Previously Presented) The system of claim 60, wherein the first node is configured to transmit a key exchange message once the server handshake completion message is received.

62. (Previously Presented) The computer readable medium of claim 46, further comprising additional instructions for performing the steps of:

setting a timer when the record is read, wherein the record is a partial record; and

clustering the partial record if the timer expires.

63. (Previously Presented) The computer readable medium of claim 62, wherein the timer corresponds to two times a packet interval time.

64. (Previously Presented) The computer readable medium of claim 46, further including the step of storing an unacknowledged portion of the data communication in a queue.

65. (Previously Presented) The computer readable medium of claim 64, wherein the data communication is stored in the queue with a cipher state associated with the record.